Как не стать жертвой мошенников при подготовке ребенка к школе

Собирают деньги в классных чатах

Многие родители уже привыкли решать школьные вопросы через мессенджеры в групповых чатах или личной переписке с педагогом. Поэтому сообщения от учителя или какого-то родителя в WhatsApp или Telegram обычно не вызывают подозрений. Так же, как и объявления на странице школы в соцсетях.

Этим пользуются мошенники. Порой им достаточно взломать аккаунт в мессенджере лишь одного родителя или учителя, чтобы получить доступ к списку контактов в классном чате. Иногда просто добавляются в чат под видом родителя новенького ученика или педагога. Либо пишут с поддельного профиля директора.

Легенда может быть любая сбор денег на экскурсию или какое-то мероприятие, просьба пройти опрос или заполнить какую-нибудь форму на субсидию. Но по факту они просят прислать деньги на свою карту или кидают фишинговую страницу. Если человек кликнет по ней, под угрозой окажутся его персональные данные, а гаджет может пострадать от вируса.

Обычно эта схема рассчитана на родителей первоклассников, которые еще не успели хорошо познакомиться друг с другом и учителем. Когда связи уже налажены, обман раскрывается довольно быстро. Но вероятность, что кто-то успеет перевести деньги мошенникам или открыть опасную ссылку, все же остается.

Бывает, что преступники создают новую группу или чат «для особых» вопросов. Например, чтобы организовать некий секретный или экстренный сбор на подарок учителю или на помощь одному из учеников. Стоит насторожиться, когда деньги собирают в срочном порядке и без предварительного обсуждения. Еще один тревожный сигнал, если перевод просят сделать на непонятный номер телефона или на карту неизвестного вам человека.

Когда вы видите в общей группе какую-то ссылку на опрос, статью о психологии школьников, курсы скорочтения, музейную экскурсию или форму заявки на льготное питание, не спешите кликать или сдавать деньги.

Проверьте, от кого пришла ссылка или информация о сборе денег, знаете ли вы этого человека, с привычного ли аккаунта он пишет. Но даже если сомнений не возникло, не повод торопиться и выполнять все указания ведь человека могли взломать.

В случае, когда вы все же прошли по ссылке, стоит насторожиться, если вас просят ввести там персональные или банковские данные, авторизоваться через соцсети или мессенджер.

Обещают несуществующие выплаты к 1 сентября

Еще одна приманка для родителей помощь в компенсации затрат на покупки к школе. Мошенники уверяют, что они помогут оформить специальную субсидию из федерального бюджета. Иногда они сразу предлагают заполнить онлайн-форму для получения выплат. И не стесняются попросить небольшую оплату за свои услуги.

Если человек доверится и выдаст информацию о себе: ФИО, СНИЛС, ИНН, номер мобильного телефона или данные карты для зачисления субсидии он сильно рискует. Мало того что никакой компенсации не будет, мошенники могут попытаться оформить онлайн-займы на его имя.

Если вам предлагают оформить какие-либо льготы, сначала проверьте, действительно ли они существуют и распространяются ли на вашу семью. Это можно выяснить на Госуслугах, в МФЦ или соцзащите.

Зазывают в поддельные магазины товаров для школы

Желание сэкономить часто затмевает глаза покупателей. Поэтому мошенники охотно создают фальшивые онлайн-магазины, где все нужное для школы якобы можно купить с большими скидками. Это могут быть любые товары для учебы, но чаще аферисты подделывают магазины школьной формы. Сделав заказ на таком сайте, вы ничего не получите, а деньги уйдут в карманы преступников. При этом можно потерять не только стоимость покупки. После того как на странице оплаты вы введете данные карты, злоумышленники постараются полностью обчистить банковский счет.

Прежде чем делать заказ в незнакомом магазине, внимательно изучите его сайт. Проверьте, кому он принадлежит, посмотрите контакты, поищите отзывы в интернете. Но даже когда выгодные цены предлагает проверенный магазин, убедитесь, что вы попали на настоящий сайт, а не на подделку.

Просят поддержать ребенка в конкурсе

Этот обман используется круглый год. Но в начале осени бывает всплеск из-за роста активности в школьных чатах. Преступники взламывают почты, аккаунты в соцсетях или мессенджерах ничего не подозревающих людей и от их имени делают рассылку по списку контактов с просьбой проголосовать за ребенка в детском конкурсе например, оценить его стишок, фотографию или рисунок. Якобы школьнику не хватает совсем немного голосов, чтобы получить приз.

Но ссылка для голосования все так же ведет на фишинговый сайт. На котором можно подцепить вирус на свой гаджет, потерять свои аккаунты в соцсетях и мессенджерах или даже открыть мошенникам доступ в свой мобильный банк.